THE CHEBOTAREV DENSITY THEOREM IN SHORT INTERVALS AND SOME QUESTIONS OF SERRE

Antal Balog and Ken Ono

Appearing in the Journal of Number Theory

1. Introduction and Statement of Results.

As usual, let $\tau(n)$ denote the coefficient of q^n ($q := e^{2\pi iz}$ throughout) in the series for

$$\Delta(z) = \sum_{n=1}^{\infty} \tau(n)q^n := q\prod_{n=1}^{\infty}(1-q^n)^{24} = q - 24q^2 + 252q^3 - 1472q^4 + \dots,$$

the unique normalized cusp form of weight 12 with respect to the full modular group. Although Lehmer's speculation that $\tau(n) \neq 0$ for every positive n remains open, Serre [S] has made substantial progress on the basic question regarding the number of Fourier coefficients of a modular form which can be zero. He shows (see [p. 179, S]) that $\tau(n)$ is non-zero for the vast majority of n.

In the same paper, Serre proposes the study of the nonvanishing of Fourier coefficients in short intervals. In particular, if

$$f(z) = \sum_{n=1}^{\infty} a_f(n)q^n \tag{1.1}$$

is in $S_k(\Gamma_0(N), \chi)$, then he suggests the problem of finding upper bounds for the function $i_f(n)$ defined by

$$i_f(n) := \max\{\ i\ :\ a_f(n+j) = 0 \text{ for all } 0 \leq j \leq i\}. \tag{1.2}$$

Serre proved [p. 183, S] that if $f(z)$ is a cusp form with integer weight $k \geq 2$ which is not a linear combination of forms with complex multiplication, then

$$i_f(n) \ll n. \tag{1.3}$$

In view of this estimate, he poses the following questions [p. 183, S]:

1991 *Mathematics Subject Classification.* Primary 11F30; Secondary 11R45.

The second author is supported by NSF grant DMS-9874947, an Alfred P. Sloan Foundation Research Fellowship, and a David and Lucile Packard Research Fellowship.

Serre's Questions. *Assume the notation above.*

1. *Suppose that $f(z)$ is a non-zero cusp form with integer weight ≥ 2 which is not a linear combination of forms with complex multiplication. Can estimate* (1.3) *be improved to an estimate of the form*

$$i_f(n) \ll_{f,m} \frac{n}{\log(n)^m} \qquad \text{for all } m \geq 0,$$

or one of the form

$$i_f(n) \ll_f n^{\delta} \qquad \text{where } 0 < \delta < 1?$$

2. *More generally, are there analogous results for forms with non-integral weights, or forms with respect to other Fuchsian groups?*

Such questions are directly related to some examples found by Knopp and Lehner [K-L]. Although these questions have not been addressed directly in the literature (to the best of our knowledge), quite a bit is known. For example, the first question follows from the classical result, due to Rankin and Selberg, that there is a positive constant A_f for which

$$\sum_{n \leq X} |a_f(n)|^2 n^{1-k} = A_f X + O(X^{3/5}).$$

It then follows that

$$i_f(n) \ll_f n^{3/5}.$$

In the present paper we consider stronger forms of Serre's questions. We seek similar short interval results with the additional property that a proportion or a 'near proportion' of the coefficients are non-zero. The first result, which pertains to Serre's first question, follows from a recent sieve result of Wu [Wu] which is based on deep analytic estimates for exponential sums by Fouvry and Iwaniec [F-I].

Theorem 1. *Suppose that $f(z) = \sum_{n=1}^{\infty} a_f(n)q^n \in S_k(\Gamma_0(N), \chi)$ is a non-zero form with integer weight $k \geq 2$ that is not a linear combination of forms with complex multiplication. For every $\epsilon > 0$ and $X^{\frac{17}{41}+\epsilon} \leq Y$ we have*

$$\#\{X < n < X+Y \ : \ a_f(n) \neq 0\} \gg_{f,\epsilon} Y.$$

In particular, we have that $i_f(n) \ll_{f,\epsilon} n^{\frac{17}{41}+\epsilon}$.

In the direction of Serre's second question, we consider weight 1 forms, half-integral weight forms, and forms which are linear combinations of forms with complex multiplication. We begin by proving a short interval version of the Chebotarev Density Theorem. This result is of independent interest.

First we fix notation. Let K be a number field and let L/K be a normal extension with Galois group $\mathrm{Gal}(L/K)$ and let $[L:\mathbb{Q}] := n_L$ and $[K:\mathbb{Q}] := n_K$. Moreover, define the constant $c(L)$ by

$$c(L) := \begin{cases} n_L & \text{if } n_L \geq 3, \\ 8/3 & \text{if } n_L = 2, \\ 12/5 & \text{if } n_L = 1. \end{cases} \tag{1.4}$$

If $\mathfrak{P}$ is a prime ideal in O_K which is unramified in O_L, then let $\left[\frac{L/K}{\mathfrak{P}}\right]$ denote the Artin symbol representing the conjugacy class of the Frobenius above $\mathfrak{P}$ in $\mathrm{Gal}(L/K)$. With these assumptions, let $\pi_C(X; L/K)$ denote

(1.5)

$$\pi_C(X; L/K) := \#\left\{\mathfrak{P} \in O_K \ : \ \mathfrak{P} \text{ unramified in } O_L, \ \left[\frac{L/K}{\mathfrak{P}}\right] = C, \text{ and } N_{K/\mathbb{Q}}(\mathfrak{P}) \leq X\right\}.$$

The Chebotarev Density Theorem asserts that as $X \to +\infty$ we have

$$\pi_C(X; L/K) \sim \frac{\#C}{\#\mathrm{Gal}(L/K)} \cdot \frac{X}{\log X}.$$

To obtain a short interval version, we follow the successful method for bounding the distance between consecutive prime numbers invented by Hoheisel, and generalized by Sokolovskiĭ[So] for prime ideals in number fields. The main ingredients of our proof are formulas for the 'prime ideal counting function' due to Lagarias and Odlyzko [L-O], and zero density estimates and zero-free regions for Dedekind zeta-functions due to Heath-Brown [HB] and Mitsui [Mi].

Theorem 2. *If $\epsilon > 0$ and $X^{1-\frac{1}{c(L)}+\epsilon} \leq Y \leq X$, then as $X \to +\infty$ we have*

$$\pi_C(X+Y; L/K) - \pi_C(X; L/K) \sim \frac{\#C}{\#\mathrm{Gal}(L/K)} \cdot \frac{Y}{\log X}.$$

We use Theorem 2 to obtain a result for coefficients in short intervals for every integer or half-integral weight cusp form with weight $\geq 3/2$ which is not a combination of the weight $3/2$ theta functions

$$\theta_{\delta,r,t}(z) = \sum_{n \equiv r \pmod{t}} n q^{\delta n^2}. \tag{1.6}$$

Since the celebrated Serre-Stark [S-S] basis theorem asserts that all weight $1/2$ modular forms are linear combinations of theta series of the form

$$\Theta_{\delta,r,t}(z) = \sum_{n \equiv r \pmod{t}} q^{\delta n^2},$$

we shall concentrate only on those half-integral weight cusp forms with weight $\geq 3/2$ which are not linear combinations of forms as in (1.6). For such forms and any integer weight cusp form we prove:

Theorem 3. *Suppose that $f(z) = \sum_{n=1}^{\infty} a_f(n)q^n \in S_k(\Gamma_0(N), \chi)$ is a non-zero cusp form with weight $1/2 < k \in \frac{1}{2}\mathbb{N}$. If $f(z)$ is not a linear combination of weight $3/2$ theta functions, then there is a positive integer k_f such that for every $\epsilon > 0$ and $X^{1-\frac{1}{k_f}+\epsilon} \leq Y \leq X$ we have*

$$\#\{X < n < X + Y \ : \ a_f(n) \neq 0\} \gg_{f,\epsilon} \frac{Y}{\log X}.$$

In particular, we have that $i_f(n) \ll_{f,\epsilon} n^{1-\frac{1}{k_f}+\epsilon}$.

We shall discuss a few corollaries regarding critical values of modular L-functions and elliptic curves. Suppose that $F(z) = \sum_{n=1}^{\infty} A(n)q^n \in S_{2k}(\Gamma_0(N), \chi_{triv})$ is an even weight newform and let $L(F, s) = \sum_{n=1}^{\infty} A(n)n^{-s}$ denote its L-function. For the remainder of this paper D shall denote the fundamental discriminant of a quadratic field. Let $L(F_D, s)$ denote the L-function given by

$$L(F_D, s) = \sum_{n=1}^{\infty} \frac{A(n)\chi_D(n)}{n^s}$$

where χ_D is the Kronecker character for $\mathbb{Q}(\sqrt{D})$. A well known conjecture due to Goldfeld [Go] asserts that $L(F_D, k) \neq 0$ for 'half' the D, and at present, the best general result in this direction (see [O-Sk]) is

$$\#\{|D| < X \ : \ L(F_D, k) \neq 0\} \gg_F \frac{X}{\log X}. \tag{1.7}$$

We obtain the following refinement of (1.7) indicating some regularity in the distribution of non-zero L-values in a family of quadratic twists.

Corollary 4. *Let $F(z) = \sum_{n=1}^{\infty} A(n)q^n \in S_{2k}(\Gamma_0(N), \chi_{triv})$ be an even weight newform. There is a positive integer k_F such that for each $\epsilon > 0$ and $X^{1-\frac{1}{k_F}+\epsilon} \leq Y \leq X$ we have*

$$\#\{X < |D| < X + Y \ : \ L(F_D, k) \neq 0\} \gg_{F,\epsilon} \frac{Y}{\log X}.$$

Let $E/\mathbb{Q}$ be a modular elliptic curve and let E_D denote its D-quadratic twist. Moreover, let $rk(E_D)$ denote the Mordell-Weil rank of E_D over $\mathbb{Q}$. We obtain:

Corollary 5. *If $E/\mathbb{Q}$ is a modular elliptic curve, then there is a positive integer k_E such that for every $\epsilon > 0$ and $X^{1-\frac{1}{k_E}+\epsilon} \leq Y \leq X$ we have*

$$\#\{X < |D| < X + Y \ : \ rk(E_D) = 0\} \gg_{E,\epsilon} \frac{Y}{\log X}.$$

V. K. Murty, M. R. Murty, Saradha, Serre and Wan have obtained estimates in the direction of the Lang-Trotter Conjecture regarding the distribution of $a_E(p)$, the traces of the

Frobenius endomorphisms of an elliptic curve $E/\mathbb{Q}$. Here we obtain estimates regarding the short interval distribution of $a_E(p) \pmod{m}$ for any given integer m. First we mention an immediate consequence of a striking result of Shiu [Shi] on consecutive primes in arithmetic progressions. Let $p_1 = 2 < p_2 = 3 < \dots$ be the primes in increasing order, and let $E/\mathbb{Q}$ be an elliptic curve with a rational point of prime order ℓ. Shiu's theorem implies for every positive integer k and each $1 \not\equiv i \pmod{\ell}$ that there is an n for which

$$a_E(p_n) \equiv a_E(p_{n+1}) \equiv a_E(p_{n+2}) \equiv a_E(p_{n+k}) \equiv i \pmod{\ell}. \tag{1.8}$$

Here we obtain a short interval result for $a_E(p) \pmod{m}$ for any integer m which indicates that strings as in (1.8), and more generally strings for any E, require that k be small compared to p_n.

Corollary 6. *Let $E/\mathbb{Q}$ be an elliptic curve, m a positive integer, and $i \pmod{m}$ a residue class for which there is a prime of good reduction p_0 with $a_E(p_0) \equiv i \pmod{m}$. There is a positive integer $k_{E,m}$ such that for every $\epsilon > 0$ and $X^{1-\frac{1}{k_{E,m}}+\epsilon} \leq Y \leq X$ we have*

$$\#\{X < p < X + Y \text{ prime } : \ a_E(p) \equiv i \mod m\} \gg_{E,\epsilon} \frac{Y}{\log X}.$$

In §2 we prove Theorem 1, and in §3 we prove Theorem 2 and in §4 we prove Theorem 3. Corollaries 4, 5, and 6 are proved in §5.

2. Proof of Theorem 1.

The general case of Theorem 1 follows from the special case for newforms, and so our first objective is to prove Theorem 1 for newforms. We begin by recalling an important fact about newforms (see [A-L, Li, M]).

Proposition 2.1. *If $f(z) = \sum_{n=1}^{\infty} a_f(n)q^n \in S_k(\Gamma_0(N), \chi)$ is an integer weight newform and m and n are coprime integers, then*

$$a_f(mn) = a_f(m)a_f(n).$$

We shall require the following important result due to Serre [p. 174, Cor. 2, S].

Lemma 2.2. *Let $f(z) = \sum_{n=1}^{\infty} a_f(n)q^n \in S_k(\Gamma_0(N), \chi)$ be an integer weight newform with weight $k \geq 2$ which does not have complex multiplication. For every $\epsilon > 0$ we have*

$$\#\{p < X \text{ prime } : \ a_f(p) = 0\} \ll_{f,\epsilon} \frac{X}{(\log X)^{\frac{3}{2}-\epsilon}}.$$

In view of Proposition 2.1 and Lemma 2.2, proving Theorem 1 in the case of newforms follows from the next result which is a special case of a theorem due to Wu [Wu].

Lemma 2.3. *Let S be a set of primes for which*

$$\#\{p \in S \text{ and } p \leq X\} \ll \frac{X}{(\log X)^{1+\delta}}$$

where $\delta > 0$. If N_S denotes the set of square-free positive integers with no prime factors in S, then for every $\epsilon > 0$ and $X^{\frac{17}{41}+\epsilon} < Y$ we have

$$\#\{X < n < X + Y \ : \ n \in N_S\} \gg_{S,\epsilon} Y.$$

Proof of Lemma 2.3. Let $\mathcal{B}$ denote a sequence of increasing integers $b_1 < b_2 < \dots$ of mutually coprime positive integers for which $\sum_{i=1}^{\infty} \frac{1}{b_i} < +\infty$. Let $N_{\mathcal{B}}$ denote the set of positive integers which contain none of the b_i as divisors. If $\epsilon > 0$ and $X^{\frac{17}{41}+\epsilon} < Y$, then a theorem of Wu [Wu] states that

$$\#\{X < n < X + Y \ : \ n \in N_{\mathcal{B}}\} \gg_{\mathcal{B},\epsilon} Y.$$

Lemma 2.3 follows immediately by defining $\mathcal{B}$ by $\mathcal{B} := \{p \in S\} \cup \{q^2 \ : \ q \notin S \text{ prime}\}$.

Q.E.D.

Now we use Lemma 2.3 to prove Theorem 1.

Proof of Theorem 1. Assume that $f(z) = \sum_{n=1}^{\infty} a_f(n)q^n$ is a newform with weight $k \geq 2$ without complex multiplication. Let S denote the set of primes

$$S := \{p \mid N \textit{ prime}\} \cup \{p \textit{ prime } : a_f(p) = 0\}.$$

By Lemma 2.2 and Lemma 2.3, we have for every $\epsilon > 0$ and $X^{\frac{17}{41}+\epsilon} < Y$ that

$$\#\{X < n < X + Y \ : \ n \in N_S\} \gg_{S,\epsilon} Y.$$

However, by Proposition 2.1 it follows immediately that all such n have the property that $a_f(n) \neq 0$. This proves Theorem 1 for newforms.

Now suppose that $f(z) = \sum_{n=1}^{\infty} a_f(n)q^n$ is an integer weight cusp form in $S_k(\Gamma_0(N), \chi)$ with weight $k \geq 2$ which is not a linear combination of forms with complex multiplication. We shall reduce the claim of Theorem 1 for $f(z)$ to the case of a single newform.

First we recall the definition of the integer weight Hecke operators. If p is prime, then the Hecke operators T_p are defined by

$$T_p \mid f(z) := \sum_{n=1}^{\infty} \left(a_f(pn) + \chi(p)p^{k-1}a_f(n/p)\right) q^n. \tag{2.1}$$

If $g_1(z), g_2(z), \dots g_s(z)$ are the weight k newforms with level dividing N, then let their Fourier expansions be given by

$$g_i(z) = \sum_{n=1}^{\infty} b_i(n) q^n. \tag{2.2}$$

Therefore, if $p \nmid N$ is prime, then we have

$$T_p \mid g_i(z) = b_i(p) g_i(z). \tag{2.3}$$

Moreover by "multiplicity one", if $i \neq j$, then there are infinitely many primes p for which $b_i(p) \neq b_j(p)$.

By the theory of newforms, $f(z)$ has a unique decomposition of the form

$$f(z) = \sum_{i=1}^{s} \sum_{\delta \mid N} \alpha_{i,\delta} g_i(\delta z) \tag{2.4}$$

where $\alpha_{i,\delta}$ are complex numbers. By hypothesis, we may without loss of generality assume that $\alpha_{1,\delta} \neq 0$ for some $\delta \mid N$ where $g_1(z)$ is a newform without complex multiplication. Moreover, let δ_1 be the smallest divisor of N for which $\alpha_{1,\delta_1} \neq 0$. Let $p_1 \nmid N$ be any prime for which $b_1(p_1) \neq b_2(p_1)$. Then consider the form

$$f_1(z) = \sum_{n=1}^{\infty} a_1(n) q^n := \ T_{p_1} \mid f(z) - b_2(p_1) f(z) = \sum_{i=1}^{s} (b_i(p_1) - b_2(p_1)) \sum_{\delta \mid N} \alpha_{i,\delta} g_i(\delta z). \tag{2.5}$$

It is clear that the cusp forms $g_2(\delta z)$ do not occur in the newform decomposition of $f_1(z)$ but $g_1(\delta_1 z)$ does appear. Moreover, by (2.1) it is easy to see that

$$a_1(n) = a_f(pn) + \chi(p) p^{k-1} a_f(n/p) - b_2(p_1) a_f(n). \tag{2.6}$$

Arguing in this way, one may inductively remove all the non-zero newform components $g_i(\delta z)$ for all $2 \leq i \leq s$ to obtain a cusp form $F(z)$ (after by dividing by the obvious non-zero scalar) in $S_k(\Gamma_0(N), \chi)$

$$F(z) = \sum_{n=1}^{\infty} A(n) q^n := \sum_{\delta \mid N} \alpha_{1,\delta} g_1(\delta z). \tag{2.7}$$

Moreover, by iterating (2.5) and (2.6) this form has the the property that there are finitely many algebraic numbers β_j and positive rational numbers γ_j for which

$$A(n) = \sum_{\delta \mid N} \alpha_{1,\delta} b_1(n/\delta) = \sum_j \beta_j a_f(\gamma_j n) \tag{2.8}$$

for all n. By applying the $U(\delta_1)$ operator which acts by

$$U(\delta_1) \mid \sum_{n=0}^{\infty} c(n)q^n := \sum_{n=0}^{\infty} c(\delta_1 n)q^n$$

we obtain a cusp form $F^*(z) = \sum_{n=1}^{\infty} A^*(n)q^n$ in $S_k(\Gamma_0(N), \chi)$ with the property that $A^*(n) = A(\delta_1 n)$ for all n.

Let S_1 denote the set of primes

$$S_1 := \{p \mid N \ prime\} \cup \{p \ prime \ : \ b_1(p) = 0\},$$

and let N_{S_1} denote the set of square-free positive integers with no prime factors in S_1. By (2.8) and the minimality of δ_1, for every integer $n \in N_{S_1}$ we have that

$$A^*(n) = \alpha_{1,\delta_1} b_1(n) = \sum_j \beta_j a_f(\gamma_j \delta_1 n).$$

Hence, for every integer $n \in N_{S_1}$ we have that $b_1(n) \neq 0$ implies that $a_f(\gamma_j \delta_1 n) \neq 0$ for at least one j. The conclusion of Theorem 1 for $f(z)$ follows immediately from the result for the newform $g_1(z)$.

Q.E.D.

3. Proof of Theorem 2.

In this section we prove Theorem 2. We begin by fixing notation. We fix an arbitrary element $g \in C$ of the conjugacy class C, and let $H = \langle g \rangle$ be the cyclic subgroup of $\mathrm{Gal}(L/K)$ generated by g. Moreover, recall the definition of $c(L)$ from (1.4). Throughout, $\sum_\chi$ (resp. $\prod_\chi$) shall denote the sum (resp. product) over all irreducible characters χ of H. Moreover, if χ is a character of H, then let $L(s, \chi)$ be its associated Hecke L-function. Instead of studying $\pi_C(X; L/K)$ directly, we study $\Psi_C(X; L/K)$, the analog of Chebyshev's function, given by

$$\Psi_C(X; L/k) := \sum_{\substack{N_{K/\mathbb{Q}}(\mathfrak{P}^m) \leq X, \\ \mathfrak{P} \text{ unramified}, \\ \left[\frac{L/K}{\mathfrak{P}}\right]^m = C}} \log(N_{K/\mathbb{Q}}(\mathfrak{P})). \tag{3.1}$$

Using the explicit formula for $\Psi_C(X; L/K)$ due to Lagarias and Odlyzko [Th. 7.1, L-O], it is easy to obtain the following result.

Lemma 3.1. *If $2 \leq T \leq X$, then*

$$\Psi_C(X; L/K) = \frac{\#C}{\#\mathrm{Gal}(L/K)} \left(X - \sum_\chi \bar{\chi}(g) \left(\sum_{\substack{\rho \\ |\gamma| \leq T}} \frac{X^\rho}{\rho} - \sum_{\substack{\rho \\ |\rho| \leq \frac{1}{2}}} \frac{1}{\rho} \right) \right) + O\left(\frac{X \log^2 X}{T} \right),$$

where the inner sums extend over the nontrivial zeros $\rho = \beta + i\gamma$ of $L(s,\chi)$, and the implied constant may depend on K and L.

If $2 \leq T \leq Y \leq X$ are fixed, then it is easy to see that

$$\left| \frac{(X+Y)^\rho - X^\rho}{\rho} \right| = \left| \int_X^{X+Y} t^{\rho-1}\, dt \right| \leq \int_X^{X+Y} t^{\beta-1}\, dt \leq YX^{\beta-1}.$$

Therefore, by Lemma 3.1 we find that

$$\begin{aligned}(3.2)\quad & \Psi_C(X+Y;L/K) - \Psi_C(X;L/K) = \\ &= \frac{\#C}{\#\mathrm{Gal}(L/K)} \left(Y - \sum_{\chi} \bar{\chi}(g) \sum_{\substack{\rho \\ |\gamma| \leq T}} \frac{(X+Y)^\rho - X^\rho}{\rho} \right) + O\left(\frac{X \log^2 X}{T} \right) = \\ &= \frac{\#C}{\#\mathrm{Gal}(L/K)} Y + O\left(\sum_{\substack{\rho \\ |\gamma| \leq T}} YX^{\beta-1} \right) + O\left(\frac{X \log^2 X}{T} \right),\end{aligned}$$

where the last sum extends to zeros of all Hecke L-functions associated to irreducible characters of H.

To prove Theorem 2, it suffices to show that main term in (3.2) dominates the two error terms for the appropriate range of Y. The first error term depends on the zeros of the Hecke L-functions, which are precisely the zeros of the Dedekind zeta-function $\zeta_L(s)$. This follows from the following fundamental identity (see [Th. 6, He]):

$$\zeta_L(s) = \prod_{\chi} L(s,\chi).$$

Consequently, it is important to have some knowledge of the distribution of the zeros of Dedekind zeta-functions. We summarize the facts we require in the following two lemmas which are obtained from the works of Heath-Brown, Mitsui, and Sokolovskiĭ (see [H-B] and [Mi] or [So]).

Lemma 3.2. *If $\epsilon > 0$, then there is a positive number $A = A(\epsilon, L)$ such that*

$$N_L(\sigma,T) = \#\{\rho : \zeta_L(\rho) = 0,\, \sigma \leq \beta \leq 1,\, |\gamma| \leq T\} \ll T^{(c(L)+\epsilon)(1-\sigma)} \log^A T$$

uniformly in $\frac{1}{2} \leq \sigma \leq 1$.

Lemma 3.3. *There are positive numbers t_0 and $B = B(L)$ such that*

$$\zeta_L(\sigma + it) \neq 0$$

whenever

$$t \geq t_0 \quad and \quad \sigma \geq 1 - \frac{B}{(\log t)^{2/3}(\log\log t)^{1/3}}.$$

Proof of Theorem 2. If $X^{1-\frac{1}{c(L)}+\epsilon} < Y < X$, then let T be

$$T := \frac{X \log^3 X}{Y}. \tag{3.3}$$

For this T the second error term in (3.2) is dominated by the main term $\dfrac{\#C}{\#\mathrm{Gal}(L/K)}Y$.

Therefore, it suffices to examine the first error term which depends on the zeros of $\zeta_L(s)$. By Lemmas 3.2 and 3.3 we have that

$$\sum_{\substack{\rho \\ |\gamma| \leq T}} YX^{\beta-1} \ll Y \log X \max_{\sigma} X^{\sigma-1} N_L(\sigma, T) \ll Y \log^{A+1} X \max_{\sigma} \left(\frac{T^{c(L)+\epsilon}}{X}\right)^{1-\sigma}, \tag{3.4}$$

where the maximums are taken over

$$\frac{1}{2} \leq \sigma \leq \sigma_X = 1 - \frac{B}{(\log X)^{2/3}(\log\log X)^{1/3}}.$$

This follows from the fact that for every $\sigma \geq \sigma_X$ we have $N_L(\sigma, T) = 0$ provided $T \leq X$ is sufficiently large. Our choice of T and Y in (3.3) implies that $\dfrac{T^{c(L)+\epsilon}}{X} \leq X^{-2\epsilon}$ and (3.4) is maximized at $\sigma = \sigma_X$. Therefore, by (3.4) the first error term in (3.2) is bounded by

$$Y \log^{A+1} X (X^{-2\epsilon})^{1-\sigma_X} \ll Y e^{-\epsilon B (\frac{\log X}{\log\log X})^{1/3}}.$$

which is dominated by the main term. Thus we have proved that

$$\Psi_C(X+Y; L/K) - \Psi_C(X; L/K) = \frac{\#C}{\#\mathrm{Gal}(L/K)} Y + O\left(\frac{Y}{\log X}\right). \tag{3.5}$$

Finally, by the Prime Ideal Theorem, the contribution of the proper powers of prime ideals is at most $X^{1/2} \log X \leq Y$ and the contribution of the prime ideals is

$$\log N_{K/\mathbb{Q}}(\mathfrak{P}) = \log X + O(1).$$

The transition from (3.5) to the statement of Theorem 2 is now straightforward.

Q.E.D.

4. Proof of Theorem 3.

We begin by proving the following result about newforms.

Theorem 4.1. *Let $f(z) = \sum_{n=1}^{\infty} a_f(n)q^n \in S_k(\Gamma_0(N), \chi)$ be a non-zero integer weight newform where the coefficients are algebraic integers in a number field K_f. Let $\mathcal{L} \in O_{K_f}$ be a prime ideal for which there is a prime $p_0 \nmid N\ell$, where the characteristic of $O_{K_f}/\mathcal{L}$ is ℓ, for which*

$$a_f(p_0) \not\equiv 0 \pmod{\mathcal{L}}.$$

Then there is a positive integer $k_{f,\mathcal{L}}$ such that for every $\epsilon > 0$ and $X^{1-\frac{1}{k_{f,\mathcal{L}}}+\epsilon} \leq Y \leq X$ we have

$$\#\{X < p < X + Y \text{ prime} \ : \ a_f(p) \not\equiv 0 \pmod{\mathcal{L}}\} \gg_{f,\mathcal{L},\epsilon} \frac{Y}{\log X}.$$

Proof of Theorem 4.1. By the work of Eichler, Shimura, Deligne, and Serre (see [D], [D-S], [Sh]) there is a finite Galois extension $L/\mathbb{Q}$ which is unramified outside ℓN and a semi-simple Galois representation

$$\rho_{f,\mathcal{L}} : \mathrm{Gal}(L/\mathbb{Q}) \to GL_2(O_{K_f}/\mathcal{L})$$

for which

$$\text{trace } \rho_{f,\mathcal{L}}(\mathrm{frob}_p) \equiv a_f(p) \pmod{\mathcal{L}} \tag{4.1}$$

for every prime $p \nmid \ell N$. Here frob_p denotes any Frobenius element for the prime p. By the Chebotarev Density Theorem and (4.1), the conjugacy class C in $\mathrm{Gal}(L/\mathbb{Q})$ containing frob_{p_0} has the property that

$$0 \not\equiv a_f(p) \equiv a_f(p_0) \pmod{\mathcal{L}}$$

for every $\mathrm{frob}_p \in C$. The result now follows immediately from Theorem 2.

Q.E.D.

Proof of Theorem 3. We shall prove Theorem 3 by considering the following two cases:

I. The case where $f(z)$ is an integer weight cusp form.
II. The case where $f(z)$ is a half-integral weight cusp form with weight $\geq 3/2$ which is not a finite linear combination of weight $3/2$ theta functions.

Case I. Suppose that $f(z) = \sum_{n=1}^{\infty} a_f(n)q^n$ is an integer weight cusp form in $S_k(\Gamma_0(N), \chi)$. Arguing as in the proof of Theorem 1, we may reduce this case to the result for newforms (i.e. Theorem 4.1). In particular, there is a newform $g_1(z) = \sum_{n=1}^{\infty} b_1(n)q^n$ and finitely many positive rational numbers γ_j and a fixed positive integer $\delta_1 \mid N$ for which every sufficiently large prime p with $b_1(p) \neq 0$ has the property that $a_f(\gamma_j \delta_1 p) \neq 0$ for at least one j. The conclusion of Theorem 3 for $f(z)$ follows immediately from Theorem 4.1.

Case II. Suppose that $f(z) = \sum_{n=1}^{\infty} a_f(n)q^n$ is a cusp form in $S_{\lambda+\frac{1}{2}}(\Gamma_0(N), \chi)$ with $\lambda \geq 1$ which is not a linear combination of weight 3/2 theta functions. If $p \nmid N$ is prime, then the Hecke operator $T(p^2)$ on this space is defined by

$$T(p^2) \mid f(z) := \sum_{n=0}^{\infty} (a_f(p^2n) + \chi(p)\left(\frac{(-1)^\lambda n}{p}\right)p^{\lambda-1}a_f(n) + \chi(p^2)p^{2\lambda-1}a_f(n/p^2))q^n. \tag{4.2}$$

Generalizing [p. 82, Sh], there is a set of eigenforms $g_1(z), g_2(z) \ldots g_s(z)$ in $S_{\lambda+\frac{1}{2}}(\Gamma_0(N), \chi)$ of the Hecke operators $T(p^2)$ for primes $p \nmid N$ with Fourier expansions

$$g_i(z) = \sum_{n=1}^{\infty} b_i(n)q^n \tag{4.3}$$

that satisfy the following two properties:

(4.4) For each $1 \leq i \leq s$ there is a square-free n coprime to N with $b_i(n) \neq 0$.

(4.5) $S_{\lambda+\frac{1}{2}}(\Gamma_0(N), \chi)$ is spanned by the forms $g_i(\delta z)$ where $\delta \mid N$.

By combining the theory of modular symbols, the Shimura correspondence, and a theorem of Waldspurger (see [G-S, M-T-T, Sh, W]), we may assume that the coefficients of each of $g_i(z)$ are algebraic integers in a number field K. Moreover, by Shimura's correspondence each $g_i(z)$ which is not a weight 3/2 theta function has the property that its eigenvalue of $T(p^2)$, for $p \nmid N$, is an eigenvalue of T_p of a fixed newform $G_i(z)$ of weight 2λ and level dividing N.

As in Case I, we have a decomposition of $f(z)$ as

$$f(z) = \sum_{i=1}^{s} \sum_{\delta \mid N} \alpha_{i,\delta} g_i(\delta z). \tag{4.6}$$

Moreover, by hypothesis we may assume that $\alpha_{1,\delta} \neq 0$ for some $\delta \mid N$ where $g_1(z)$ is not a theta function. Chose δ_1 minimally so that $\alpha_{1,\delta_1} \neq 0$.

Arguing as in Case I with the Hecke operators T_p being replaced by the operators $T(p^2)$, we can conclude that there are finitely many positive rational numbers γ_j for which

$$b_1(n) \neq 0 \ \text{ with } \gcd(n, N) = 1 \Longrightarrow a_f(\gamma_j \delta_1 n) \neq 0 \ \text{ for some } j. \tag{4.7}$$

Hence, it suffices to prove that $g_1(z)$ satisfies the conclusion of Theorem 4 where one excludes those n which are not coprime to N. By replacing $g_1(z)$ by a suitable linear combination of its twists (possibly trivial), we may without loss of generality assume that $b_1(n) = 0$ for those n which are not coprime to N and those n which are perfect squares. Since $g_1(z)$ is not a linear combination of weight 3/2 theta functions, by a theorem of

Vigneras [V] there are infinitely many square-free integers t for which $b_1(tn^2) \neq 0$ for some n. Moreover, since $g_1(z)$ is an eigenform with coefficients which are algebraic integers in a number field, by (4.2) we have that $b_1(t) \mid b_1(tn^2)$ for every n. Therefore, the minimal 2-adic valuation of the coefficients $b_1(n)$ is attained by $b_1(t_0)$ for some square-free integer t_0.

By the proof of the [Fund. Lemma, O-Sk], the minimal 2-adic behavior of the coefficients $b_1(n)$ is controlled by the Fourier expansion of some weight $\lambda+1$ cusp form. The trick is simply to multiply $g_1(z)$ by $\theta(z) = 1 + 2q + 2q^4 + \cdots \equiv 1 \pmod 2$. Using $b(t_0)$ in [Fund. Lemma, O-Sk], we find that the conclusion of Theorem 3 for $g_1(z)$ follows immediately from Case I. The result for $f(z)$ follows easily from (4.7).

Q.E.D.

5. Proofs of Corollaries.

Here we prove the corollaries described in the introduction.

Proofs of Corollaries 4 and 5. Both results follow from Theorem 3 on the nonvanishing of the Fourier coefficients in the case of half-integral weight cusp forms. The works of Shimura and Waldspurger [Sh2, W] shows that the coefficients of a half-integral weight cusp form $g(z)$, which is an eigenform but not a theta function, interpolates many central critical values of the quadratic twists of the modular L-function associated to the Shimura correspondent of $g(z)$. Although the Shimura correspondence is not surjective, it is shown in [§2, O-Sk] that such critical values can be obtained in this way for every modular L function of an even weight newform with trivial Nebentypus.

Corollary 5 is an immediate consequence of Corollary 4, the fact that the L-function of E_D is the D-quadratic twist of $L(E,s)$ when $\gcd(D,4N)=1$, and the celebrated theorem of Kolyvagin that [Ko]

$$L(E,1) \neq 0 \Longrightarrow rk(E) = 0.$$

Q.E.D.

Proof of Corollary 6. This result follows immediately from Theorem 2 and the mere definition of the action of Galois on the torsion points of an elliptic curve E.

Q.E.D.

References

[A-L] A. O. L. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Math. Ann. **185** (1970), 134-160.

[D] P. Deligne, *Formes modulaires et reṕresentations ℓ-adiques*, Seminaire Bourbaki **355** (1969).

[D–S] P. Deligne and J.-P. Serre, *Formes modulaires de poids 1*, Ann. Sci. École Normale Sup. 4^e sér. 7 (1974), 507-530.

[F-I] E. Fouvry and H. Iwaniec, *Exponential sums with monomials*, J. Number Theory **33** (1989), 311-333.

[Go] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Number Theory, Carbondale, Springer Lect. Notes 751 (1979), 108-118.

[G-S] R. Greenberg and G. Stevens, *On the conjecture of Mazur, Tate and Teitelbaum*, p-adic monodromy and the Birch and Swinnerton-Dyer Conjecture [B. Mazur and G. Stevens, Eds.], Cont. Math. **165** (1994), 183-211.

[H-B] D. R. Heath-Brown, *On the density of the zeros of the Dedekind zeta function*, Acta Arith. **33** (1977), 169-181.

[He] H. Heilbronn, *Zeta functions and L-functions*, In: Algebraic Number Theory [J. W. S. Cassels and A. Frölich, eds], Academic Press, New York, London (1967), 204-230.

[K-L] M. I. Knopp and J. Lehner, *Gaps in the Fourier series of automorphic forms*, Analytic Number Theory, (Philadelphia, Pa. 1980) Springer Lect. Notes in Math. **899** (1981), 360-381.

[Ko] V. Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and $Ш_{E/\mathbb{Q}}$ for a subclass of Weil curves (Russian)*, Izv. Akad. Nauk. USSR, ser. Matem. **52** (1988), 522-540.

[L-O] J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, 1975) (1977), Academic Press, London, 409-464.

[M-T-T] B. Mazur, J. Tate, J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), 1-48.

[Li] W.-C. Li, *Newforms and functional equations*, Math. Ann. **212** (1975), 285-315.

[Mi] T. Mitsui, *On the prime ideal theorem*, J. Math. Soc. Japan **20** (1968), 233-247.

[M] T. Miyake, *On automorphic forms on GL_2 and Hecke operators*, Ann. of Math. **94** (1971), 174-189.

[O-Sk] K. Ono and C. Skinner, *Non-vanishing of quadratic twists of modular L-functions*, Invent. Math. **134** (1998), 651-660.

[S] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. **54** (1981), 323-401.

[S-S] J.-P. Serre and H. Stark, *Modular forms of weight $\frac{1}{2}$*, Springer Lect. Notes 627 (1977), 27-67.

[Sh] G. Shimura, *Introduction to the arithmetic theory of automrphic functions*, Iwanami Shoten and Princeton Univ. Press, 1971.

[Sh2] G. Shimura, *On modular forms of half-integral weight*, Annals of Math. **97** (1973), 440-481.

[Shi] D. Shiu, *Strings of congruent primes*, to appear, J. London Math. Soc.

[So] A. V. Sokolovskiĭ, *A theorem on the zeros of Dedekind's zeta-function and the distance between "neighbouring" prime ideals (Russian)*, Acta Arith. **13** (1968), 321-334.

[V] M.-F. Vignéras, *Facteurs gamma et équations fonctionelles*, Modular functions of one variable, VI (Proc. Second Int. Conf., Univ. Bonn, 1976), Springer Lect. Notes Math. **627** (1977), 79-103.

[W] J.-L. Waldspurger, *Sur les coefficients de Fourier des formes modulaire de poids demi-entier*, J. Math. Pures et Appl. **60** (1981), 375-484.

[Wu] J. Wu, *Nombres $\mathcal{B}$-libres dans les petites intervalles*, Acta Arith. **65** (1993), 97-116.

Mathematical Institute of the Hungarian Academy of Sciences, P.O. Box 127, Budapest 1364, Hungary

E-mail address: `balog@hexagon.renyi.hu`

Dept. Math., University of Wisconsin, Madison, Wisconsin, 53706, USA.

E-mail address: `ono@math.wisc.edu`